FOTO90" 60527860

FIG. 1

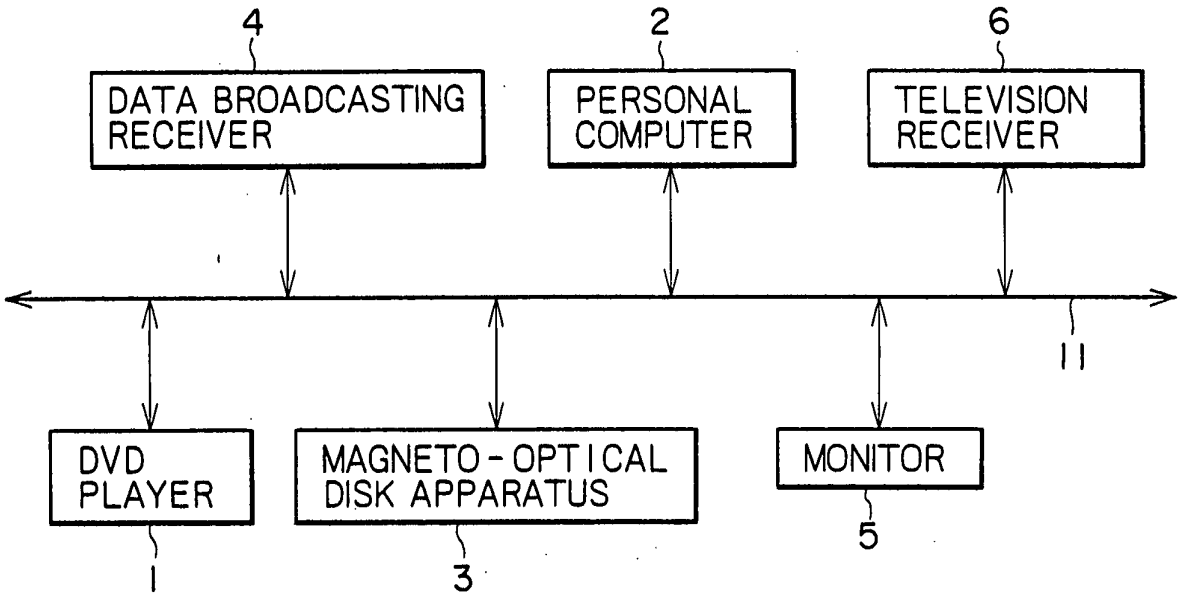


FIG. 2

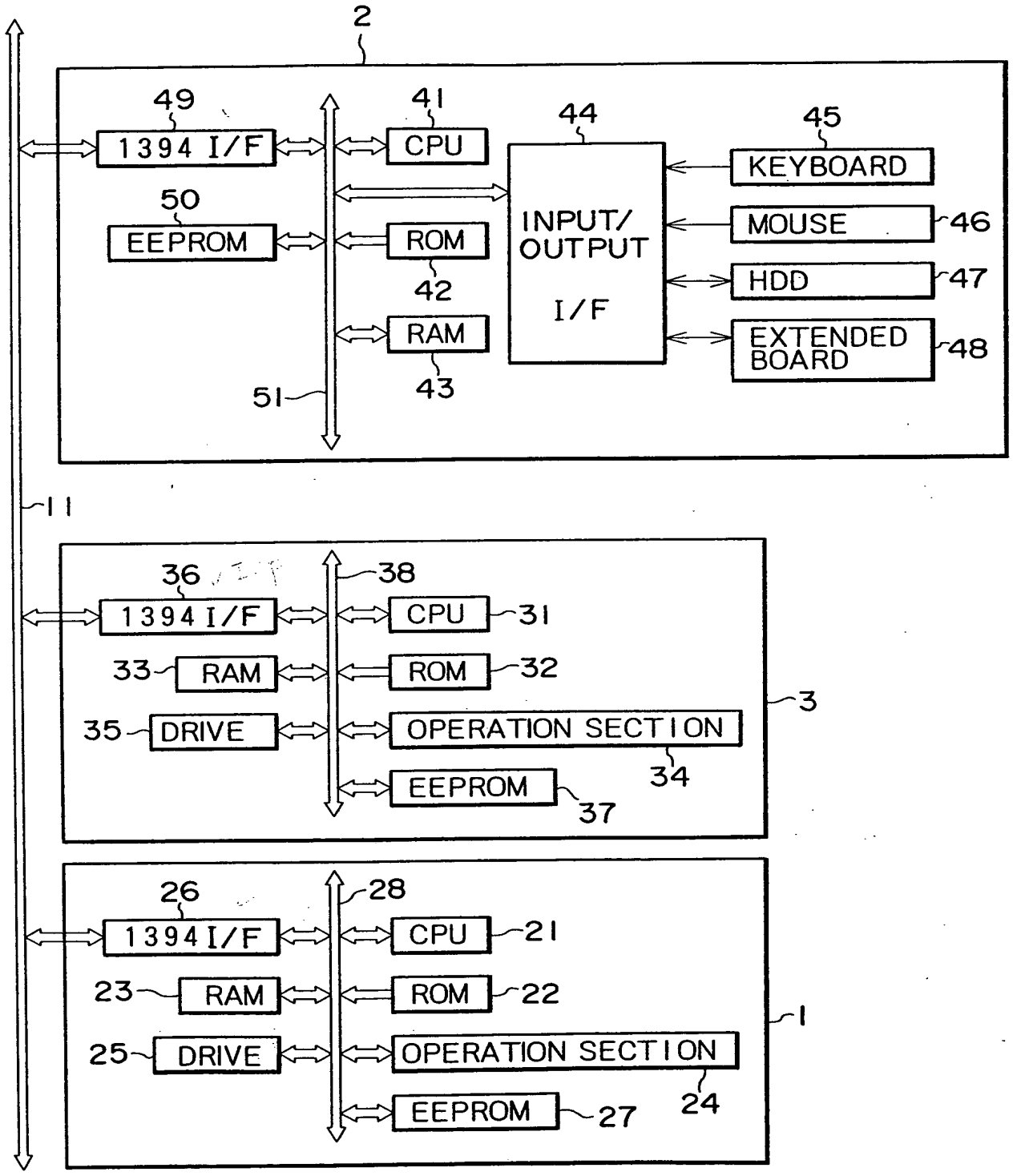

2
49
1394 I/F
41
CPU
44
INPUT/
OUTPUT
I/F
45
KEYBOARD
MOUSE
46
HDD
47
EXTENDED
BOARD
48
50
EEPROM
ROM
42
RAM
43
51
11
36
1394 I/F
38
CPU
31
33
RAM
ROM
32
35
DRIVE
OPERATION SECTION
34
EEPROM
37
3
26
1394 I/F
28
CPU
21
23
RAM
ROM
22
25
DRIVE
OPERATION SECTION
24
EEPROM
27
1

FIG. 3

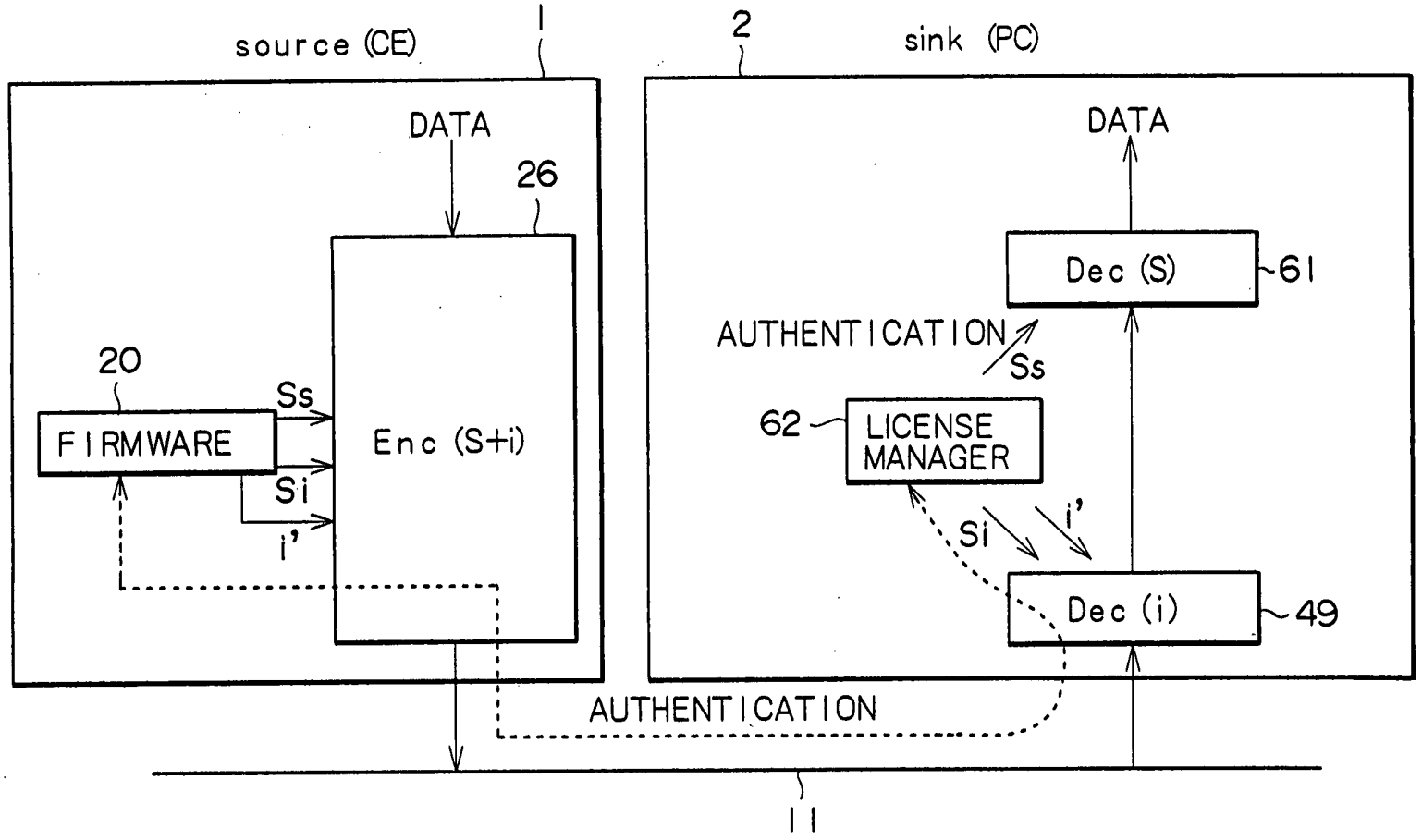

source (CE)
1
2
sink (PC)
DATA
26
DATA
Dec (S)
61
AUTHENTICATION
Ss
20
Ss
FIRMWARE
Enc (S+i)
62
LICENSE MANAGER
Si
i'
Si
i'
Dec (i)
49
AUTHENTICATION
11

FIG. 4

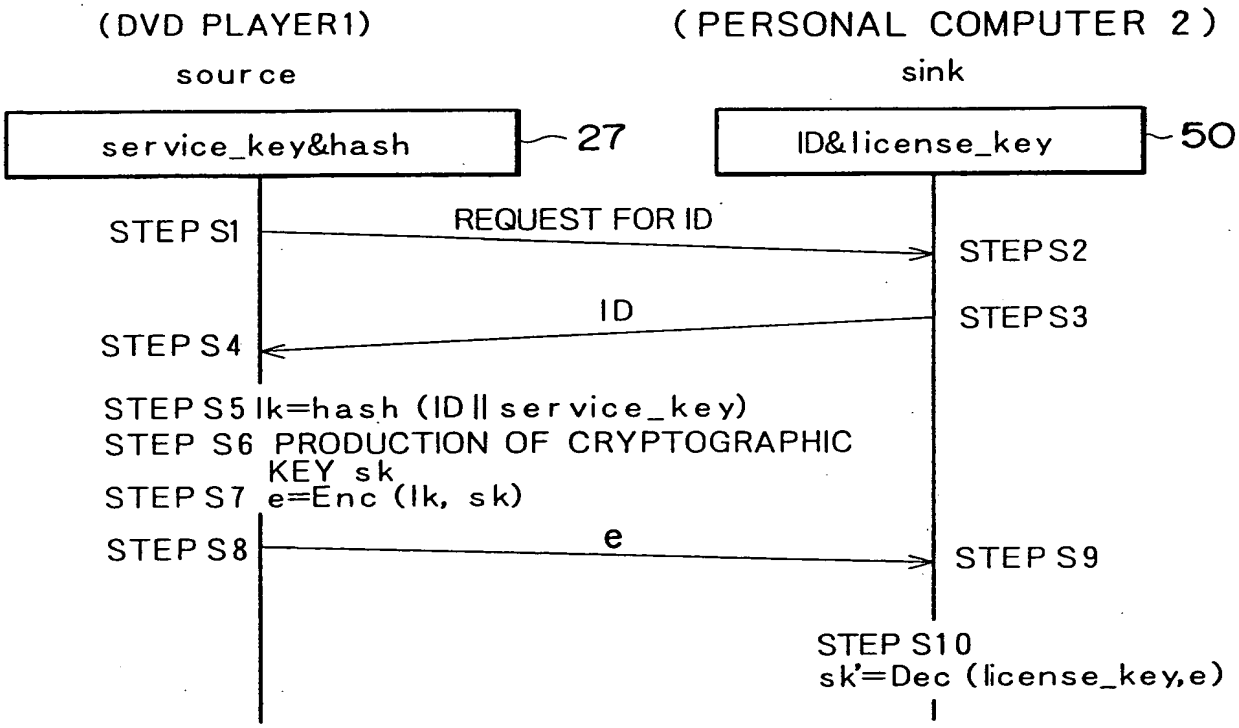
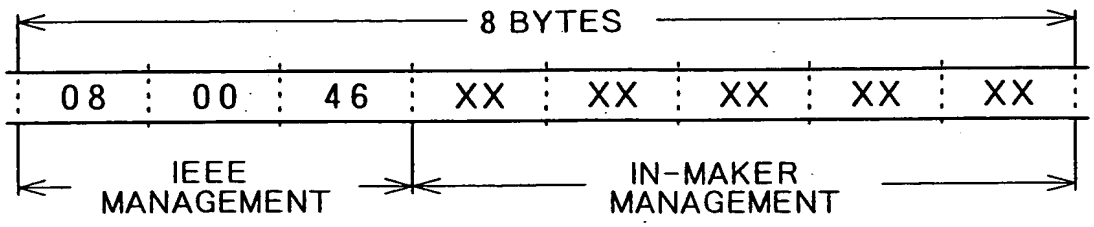
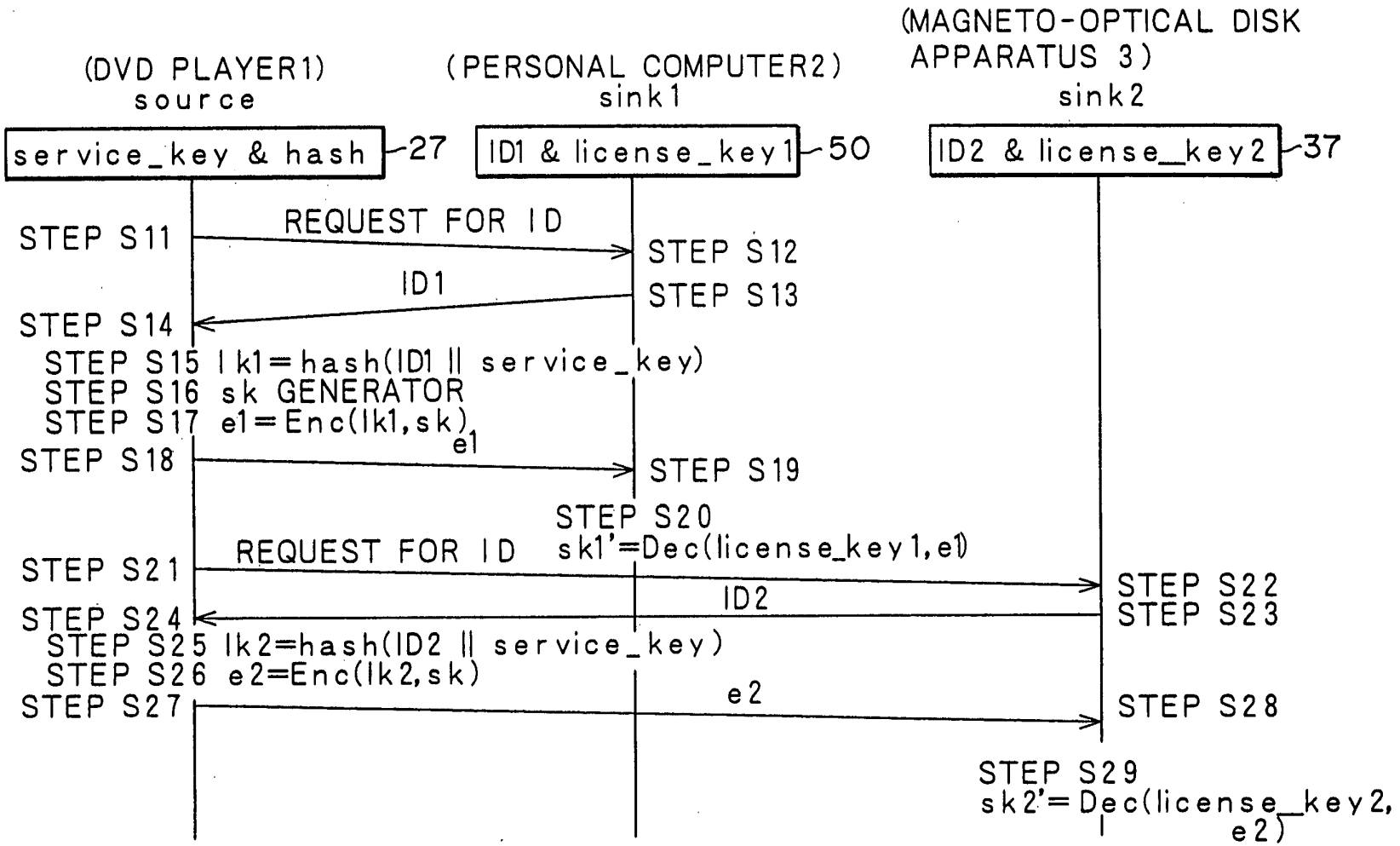

(DVD PLAYER1)
source
(PERSONAL COMPUTER 2)
sink
service_key&hash
27
ID&license_key
50
STEP S1
REQUEST FOR ID
STEP S2
ID
STEP S3
STEP S4
STEP S5 Ik=hash (ID || service_key)
STEP S6 PRODUCTION OF CRYPTOGRAPHIC KEY sk
STEP S7 e=Enc (Ik, sk)
STEP S8
e
STEP S9
STEP S10
sk'=Dec (license_key,e)

FIG. 5


8 BYTES
08
00
46
XX
XX
XX
XX
XX
IEEE MANAGEMENT
IN-MAKER MANAGEMENT

TOTO90"60527860

FIG. 6



JP090"60527860

FIG. 7

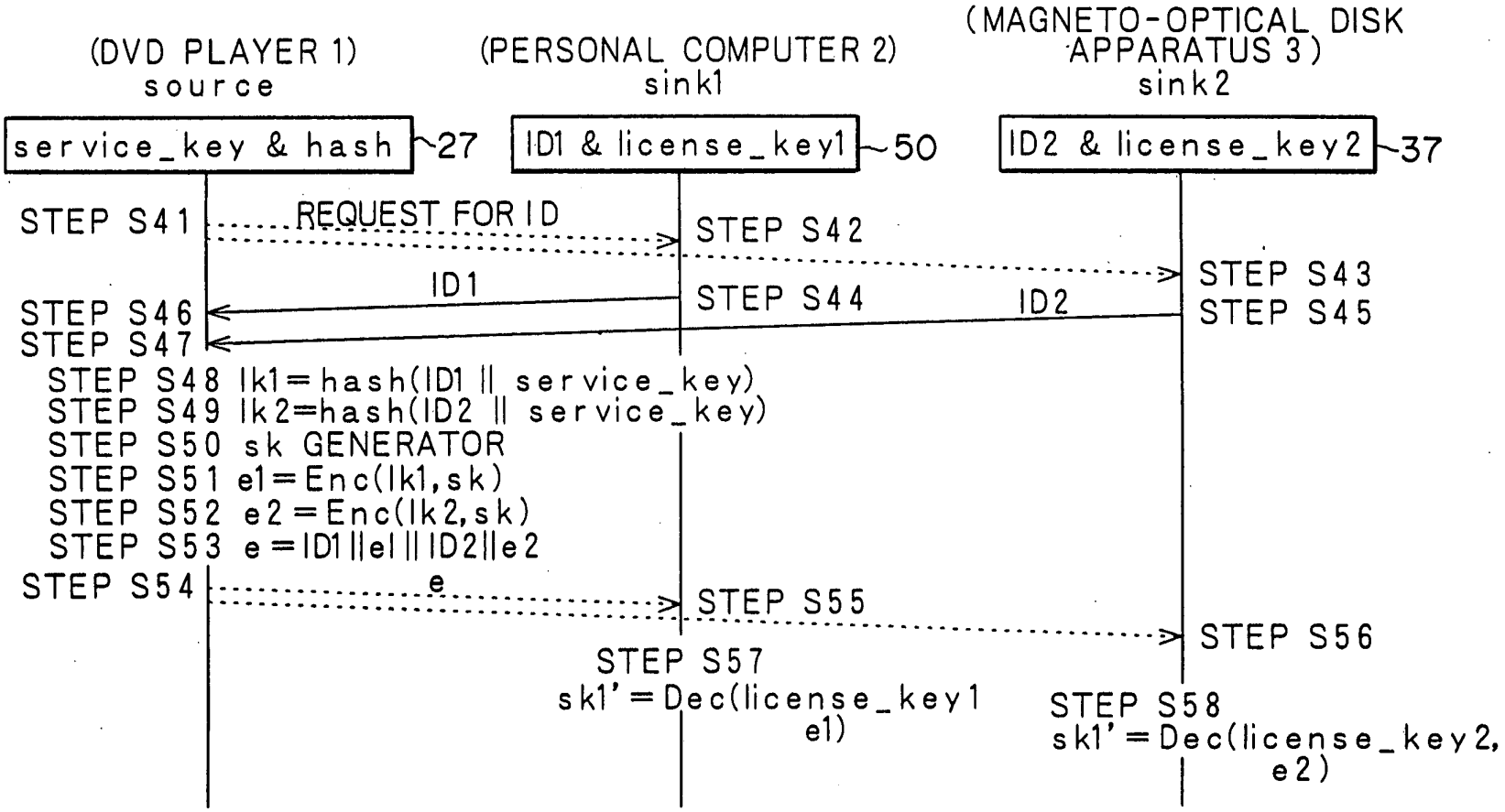


FIG. 8

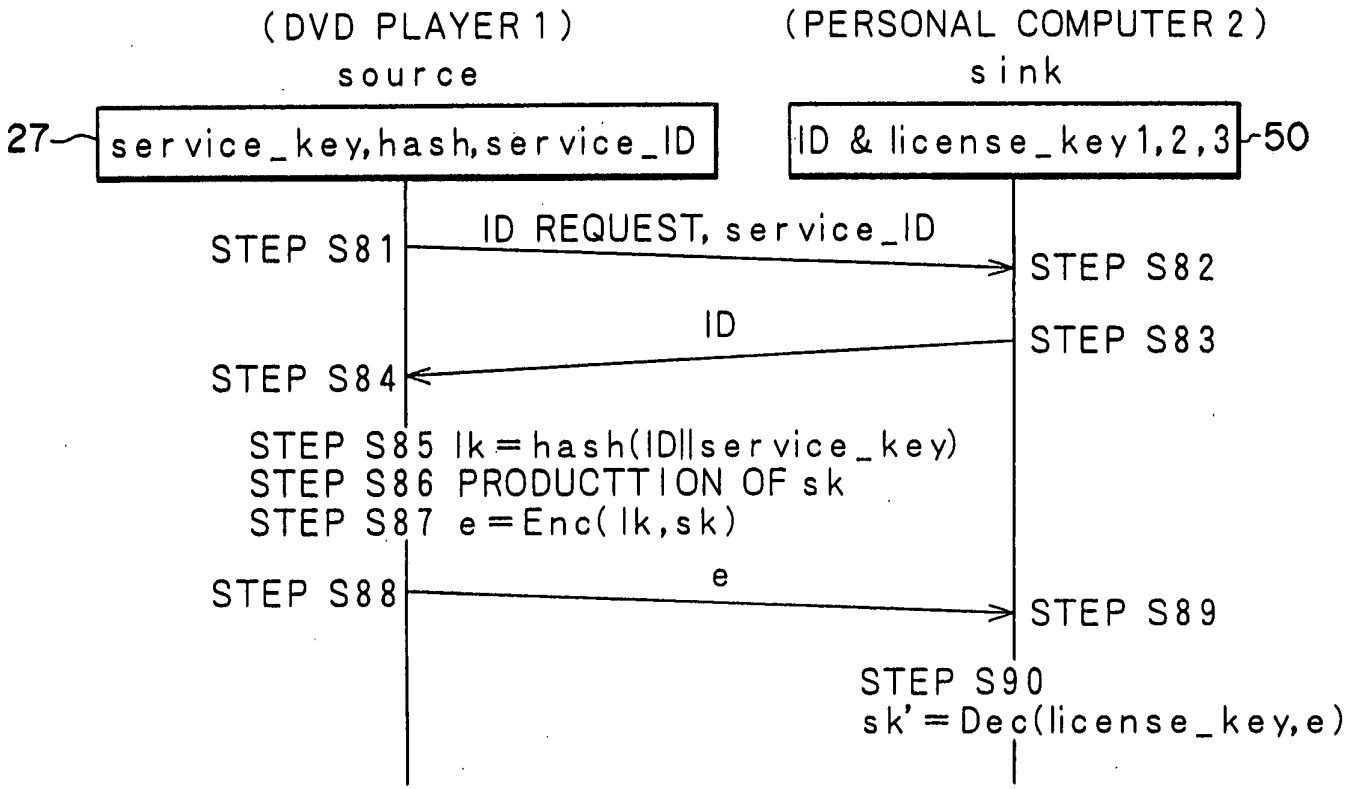

(DVD PLAYER 1)
source
(PERSONAL COMPUTER 2)
sink
27
service_key,hash,service_ID
ID & license_key1,2,3
50
STEP S81
ID REQUEST, service_ID
STEP S82
ID
STEP S83
STEP S84
STEP S85 lk=hash(ID||service_key)
STEP S86 PRODUCTTION OF sk
STEP S87 e=Enc(lk,sk)
e
STEP S88
STEP S89
STEP S90
sk'=Dec(license_key,e)

FIG. 9

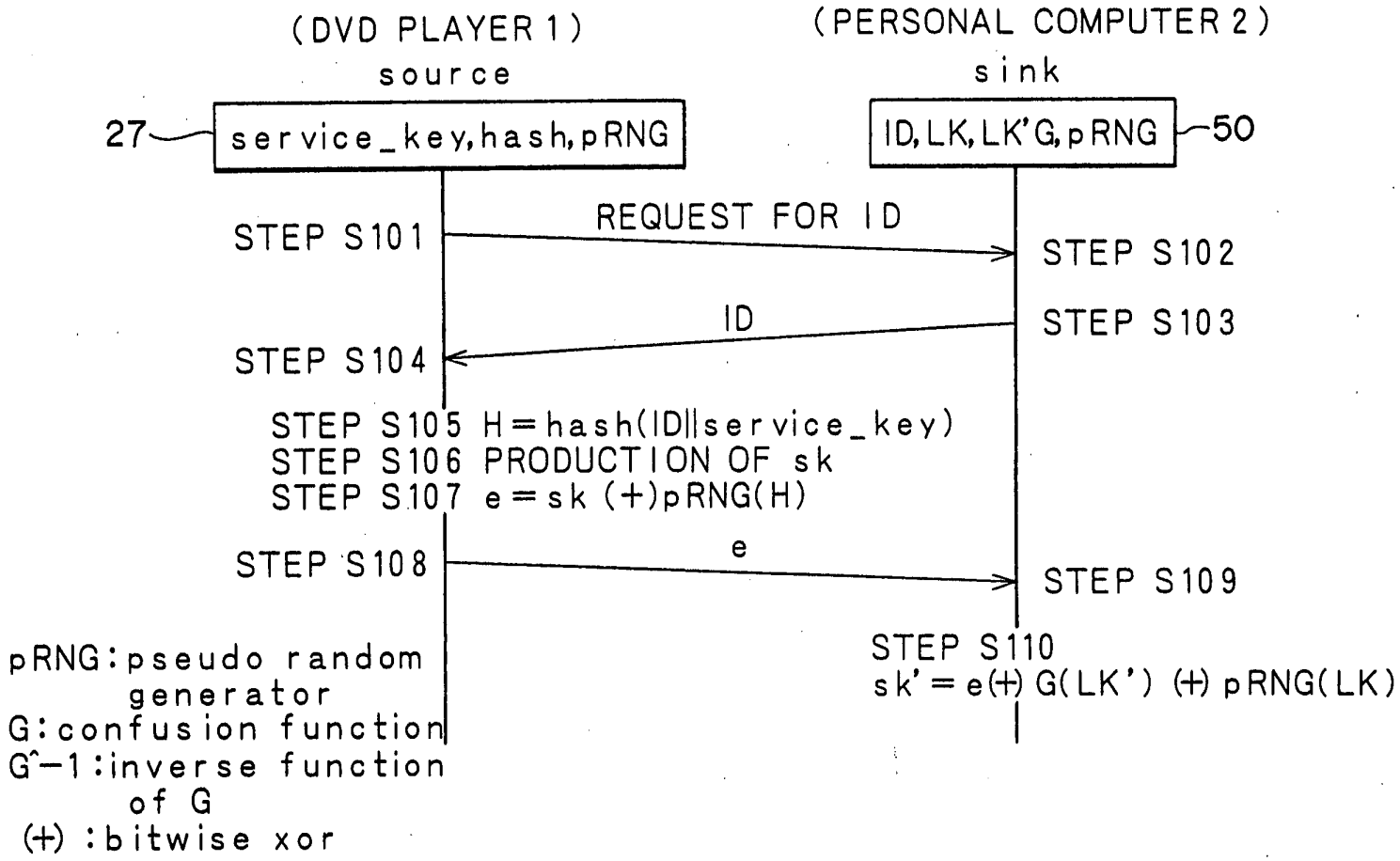
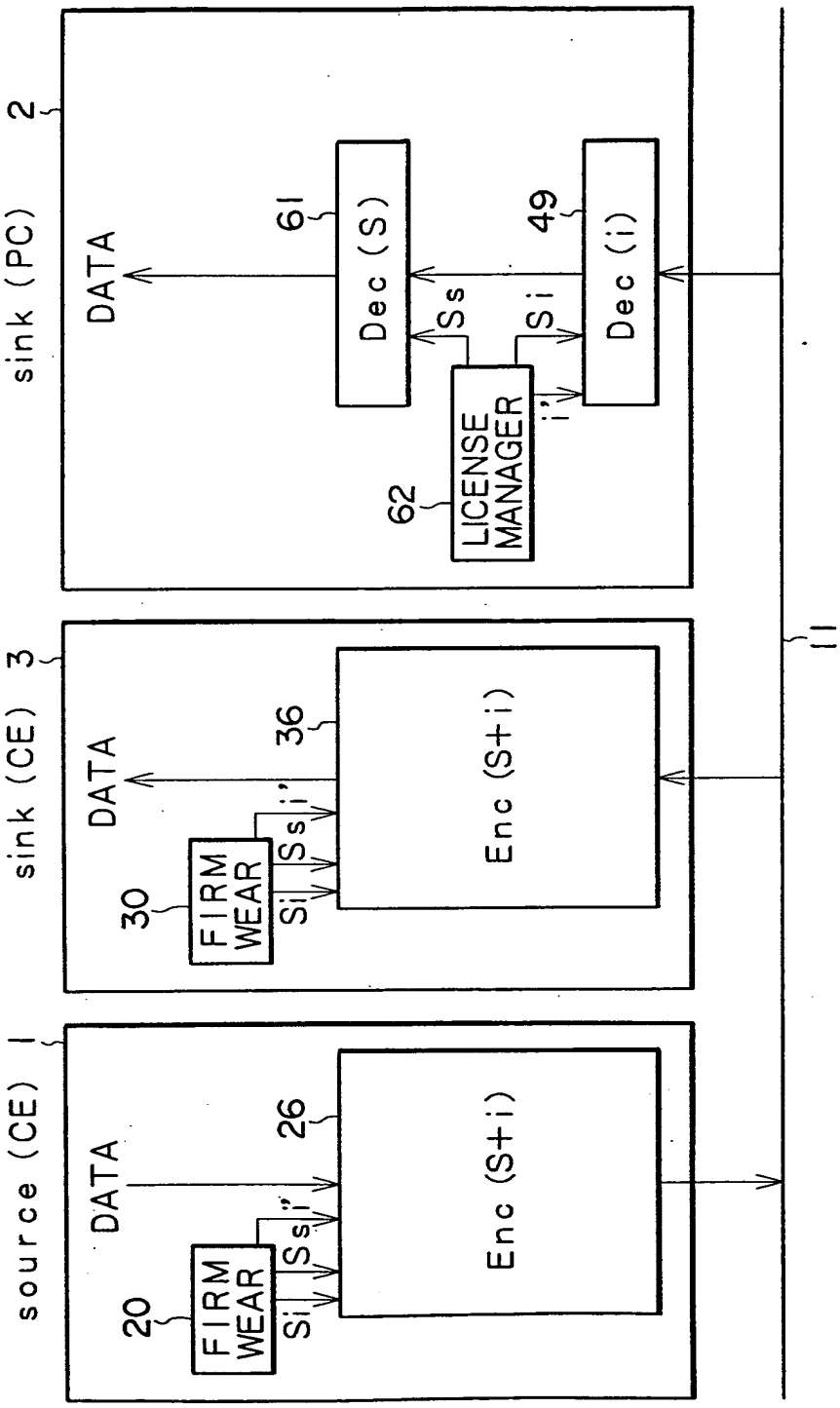

(DVD PLAYER 1)
source
(PERSONAL COMPUTER 2)
sink
27
service_key, hash, pRNG
ID, LK, LK'G, pRNG
50
REQUEST FOR ID
STEP S101
STEP S102
ID
STEP S103
STEP S104
STEP S105 H=hash(ID||service_key)
STEP S106 PRODUCTION OF sk
STEP S107 e=sk (+)pRNG(H)
e
STEP S108
STEP S109
STEP S110
sk'=e(+) G(LK') (+) pRNG(LK)
pRNG: pseudo random generator
G: confusion function
G^-1: inverse function of G
(+) : bitwise xor

FIG. 10


source (CE) 1
DATA
26
Enc (S+i)
20
FIRM WEAR
Si
Ssi'
sink (CE) 3
DATA
36
Enc (S+i)
30
FIRM WEAR
Si
Ssi'
sink (PC) 2
DATA
61
Dec (S)
49
Dec (i)
Ss
Si
i'
62
LICENSE MANAGER
11

JP090"60527860

FIG. 11

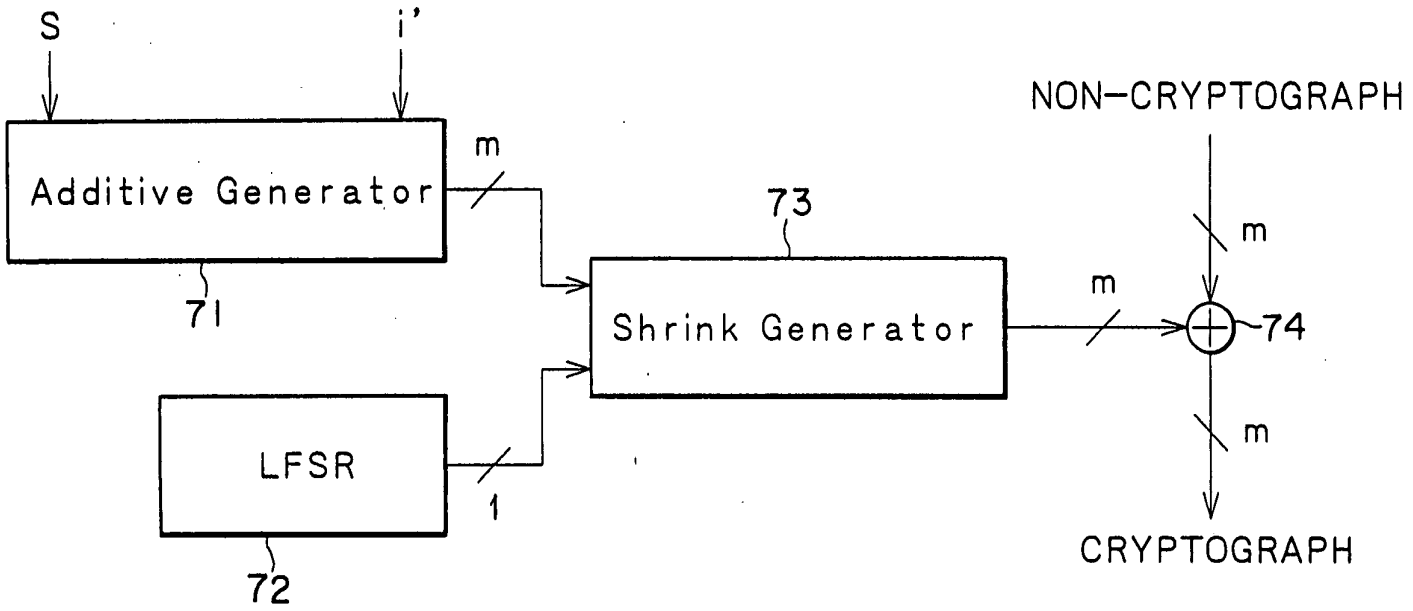


FIG. 12

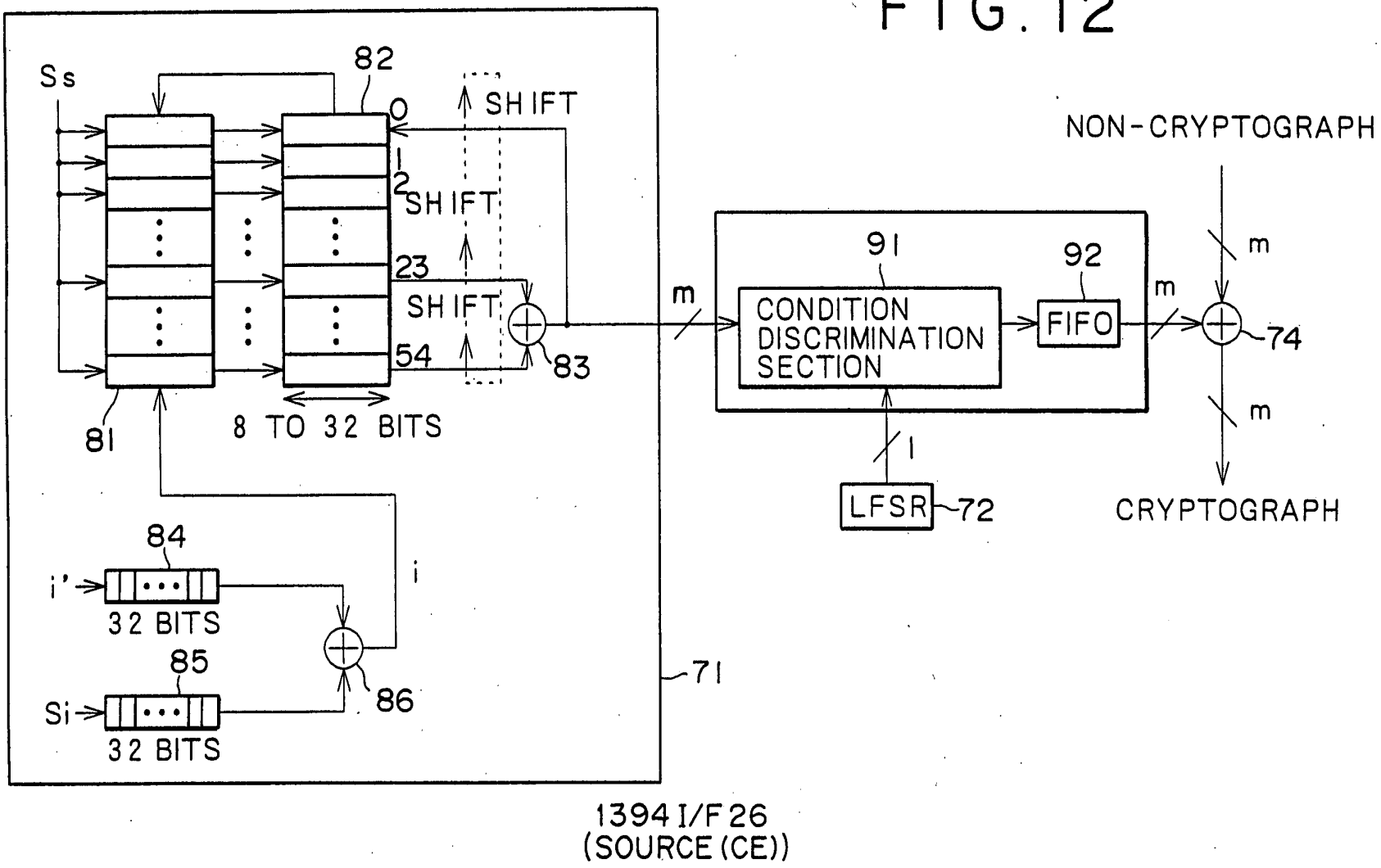
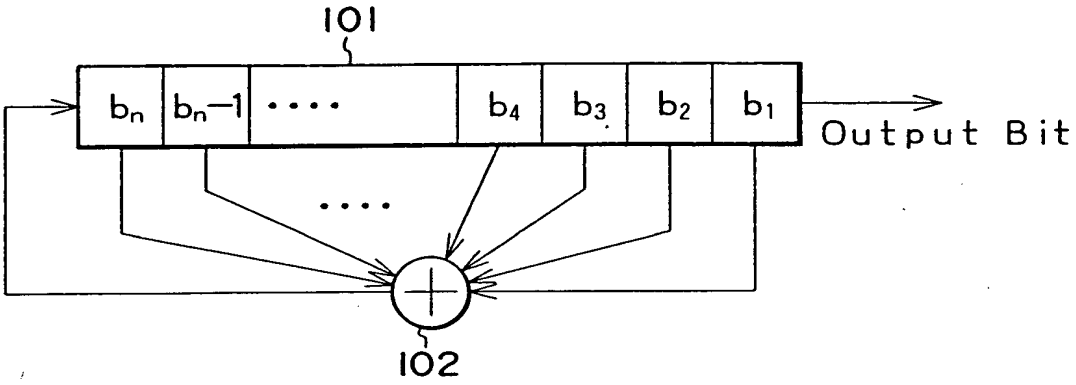
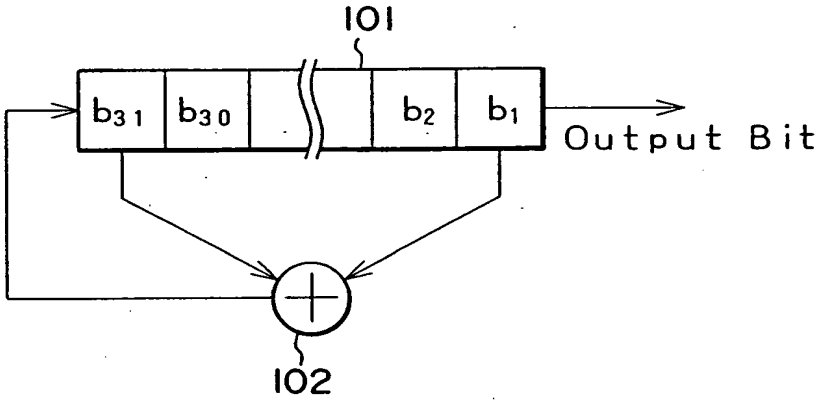

Ss
82
0
1
2
SHIFT
SHIFT
23
SHIFT
54
83
81
8 TO 32 BITS
84
i'
32 BITS
85
Si
32 BITS
86
i
71
m
91
CONDITION DISCRIMINATION SECTION
92
FIFO
m
m
74
m
1
LFSR
72
NON-CRYPTOGRAPH
CRYPTOGRAPH
1394 I/F 26
(SOURCE (CE))

FIG. 13



LFSR72

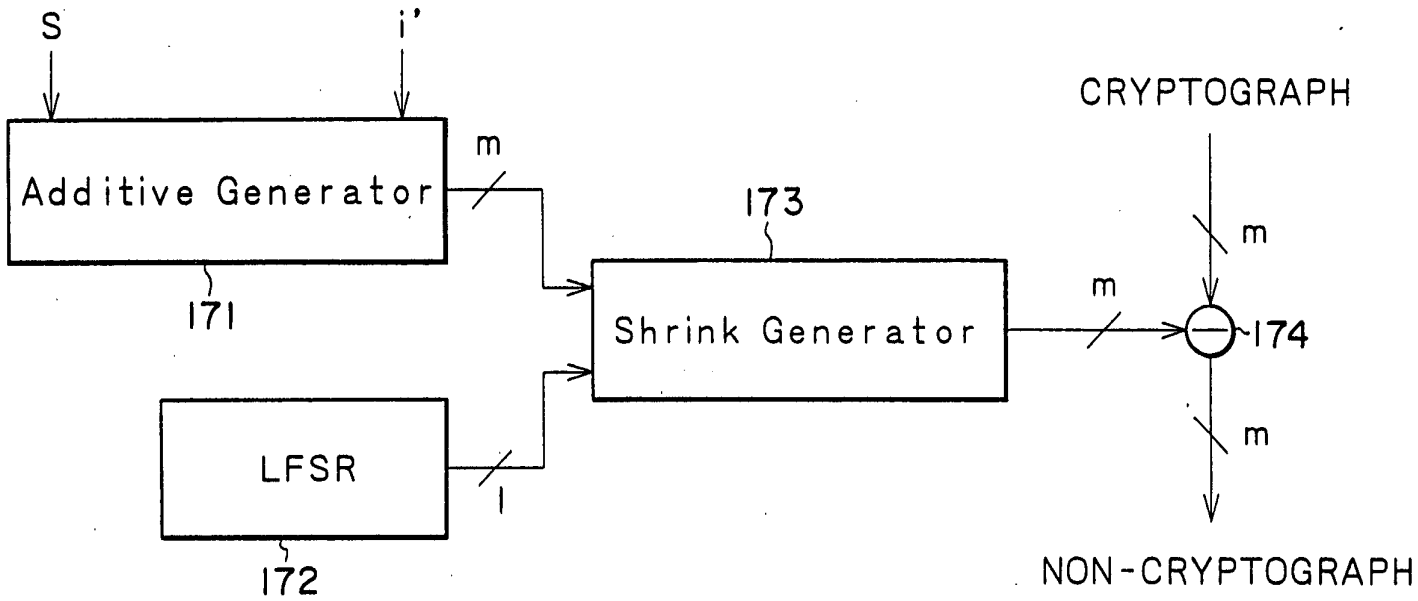
FIG. 14



LFSR72

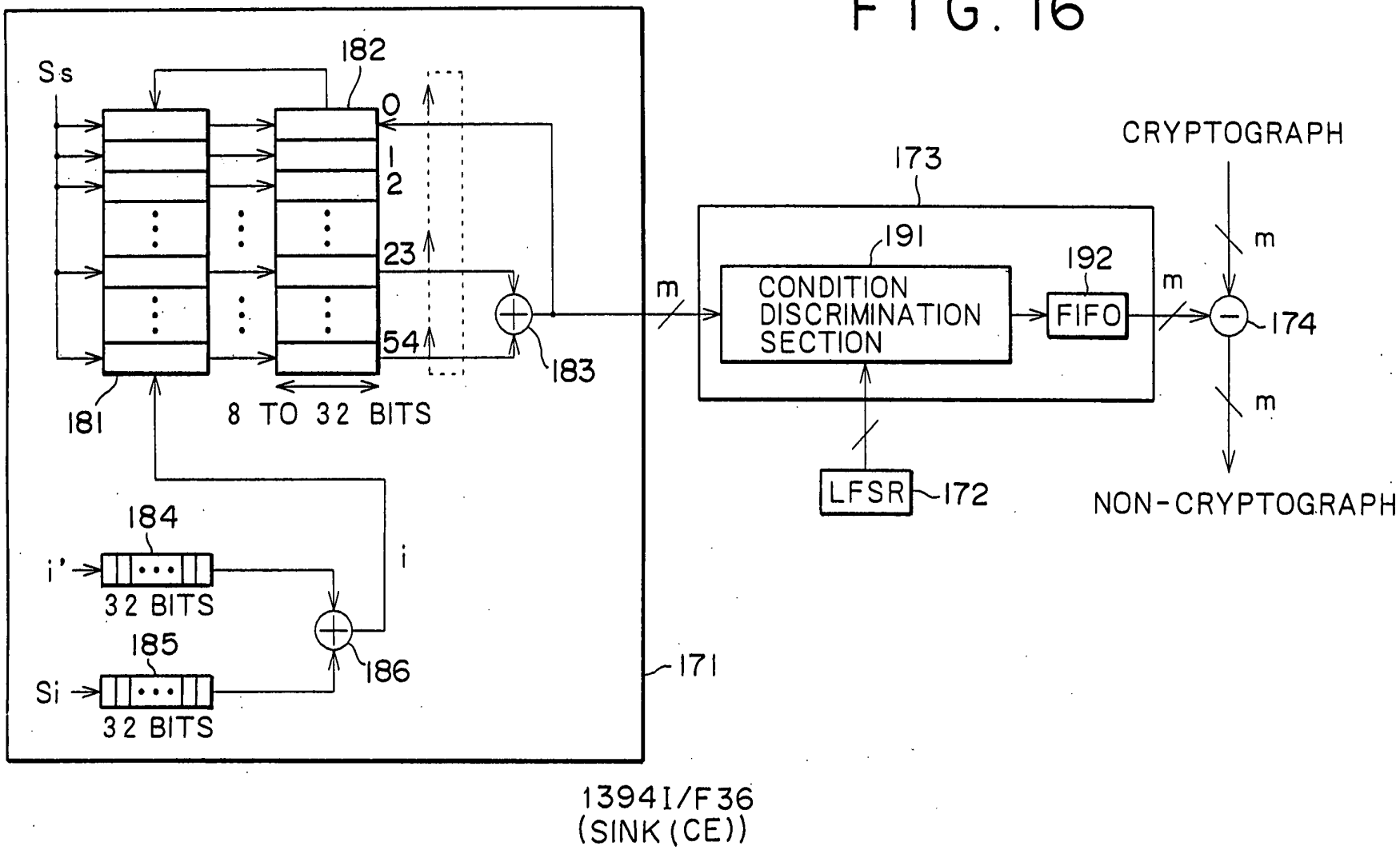
0987250-060101

FIG. 15



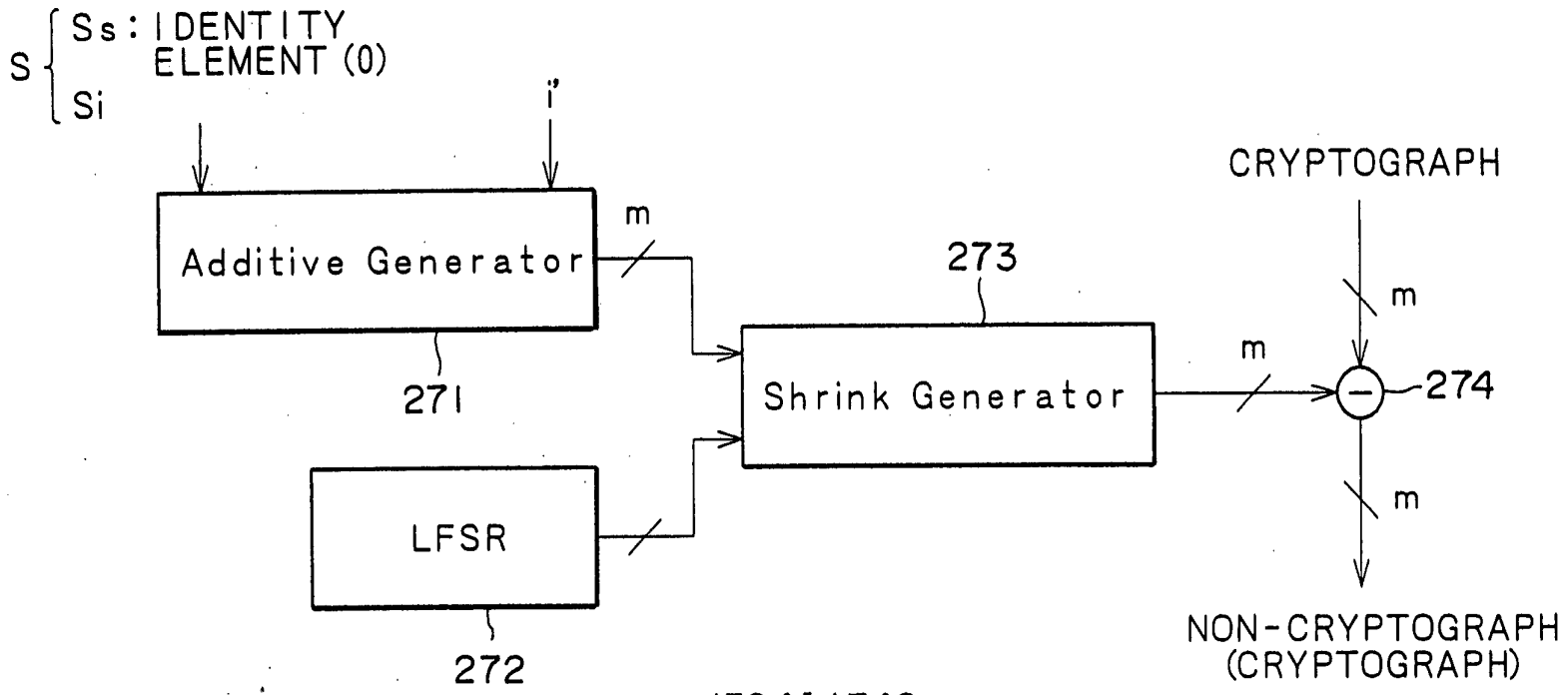
1394 I/F 36
(SINK (CE))

FIG. 16


Ss
182
0
1
2
23
54
183
181
8 TO 32 BITS
184
i'
32 BITS
185
Si
32 BITS
186
i
171
m
173
191
CONDITION DISCRIMINATION SECTION
192
FIFO
m
174
m
m
CRYPTOGRAPH
NON-CRYPTOGRAPH
LFSR
172
1394I/F36
(SINK(CE))

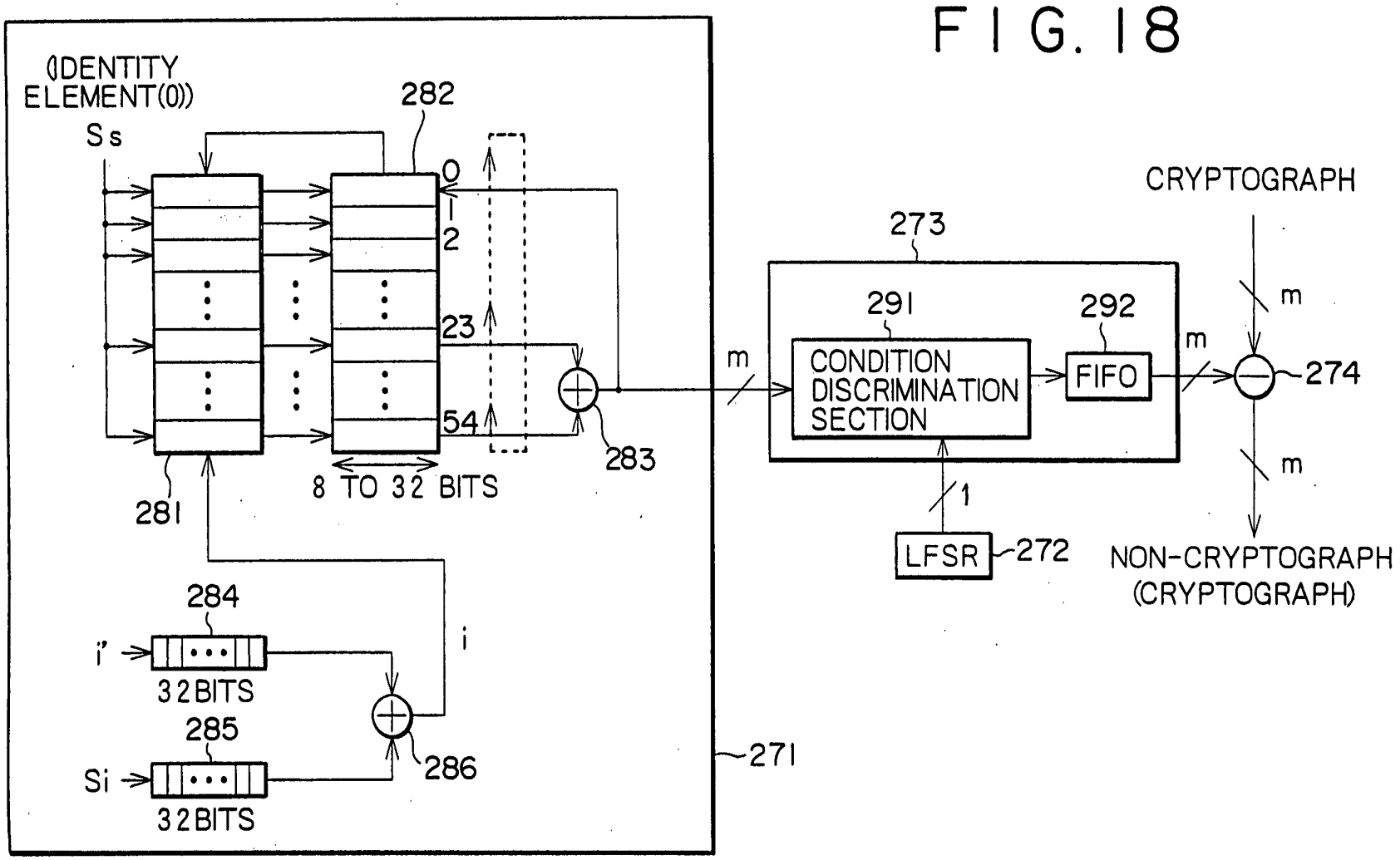
TOTO90" 60527860

FIG. 17



13941/F49
(LINK PORTION OF SINK(PC))

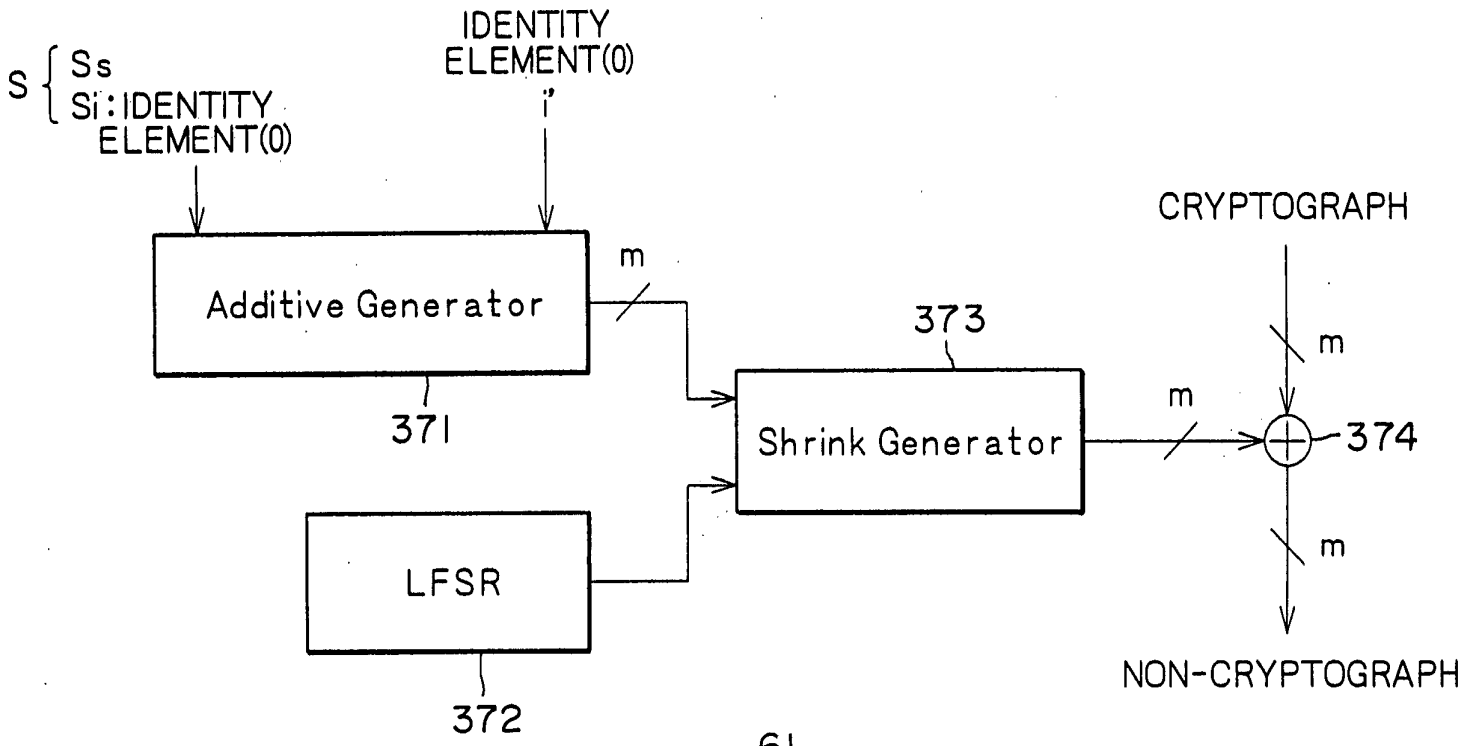
FIG. 18



1394I/F49
(LINK PORTION OF SINK(PC))

EP0190860

FIG. 19



61

EP0790760A2

FIG. 20

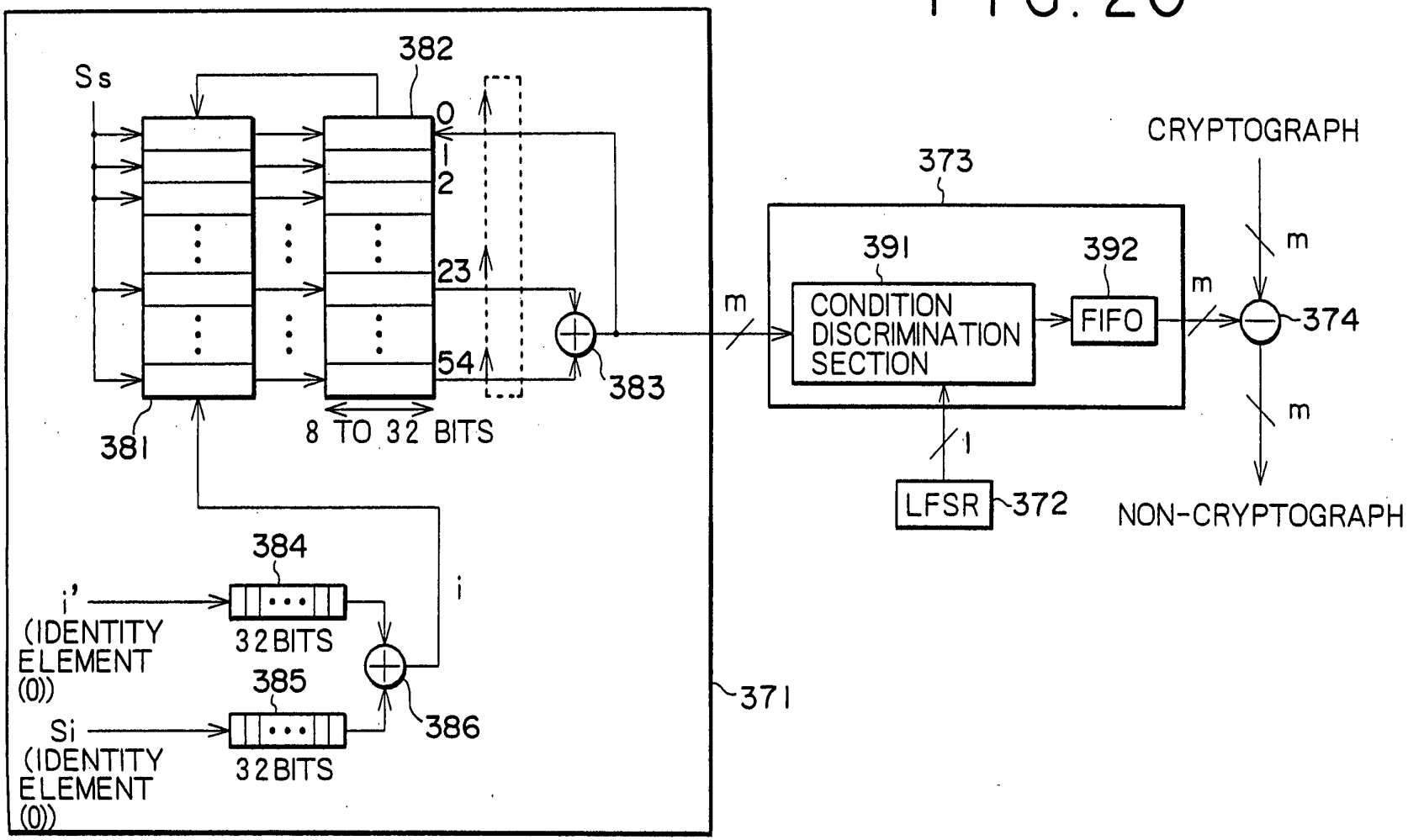
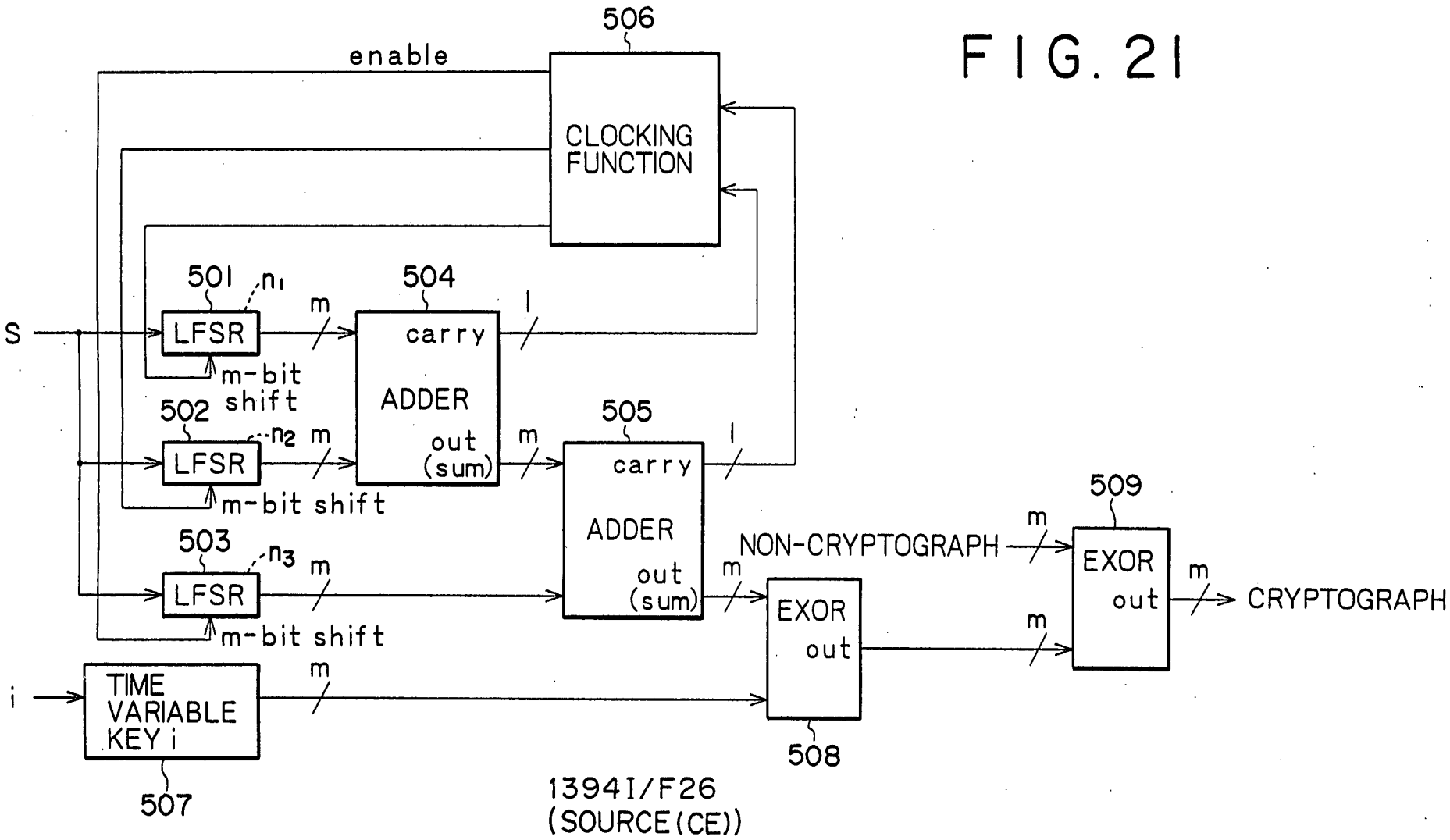


FIG. 21


506
enable
CLOCKING FUNCTION
501
n_1
504
S
LFSR
m
carry
ADDER
out (sum)
l
m-bit shift
502
n_2
505
LFSR
m
carry
ADDER
out (sum)
l
m-bit shift
509
503
n_3
NON-CRYPTOGRAPH
m
EXOR out
m
LFSR
m
m
CRYPTOGRAPH
m-bit shift
EXOR out
i
TIME VARIABLE KEY i
m
508
507
1394I/F26
(SOURCE(CE))

TOTO90"60527860

FIG. 22

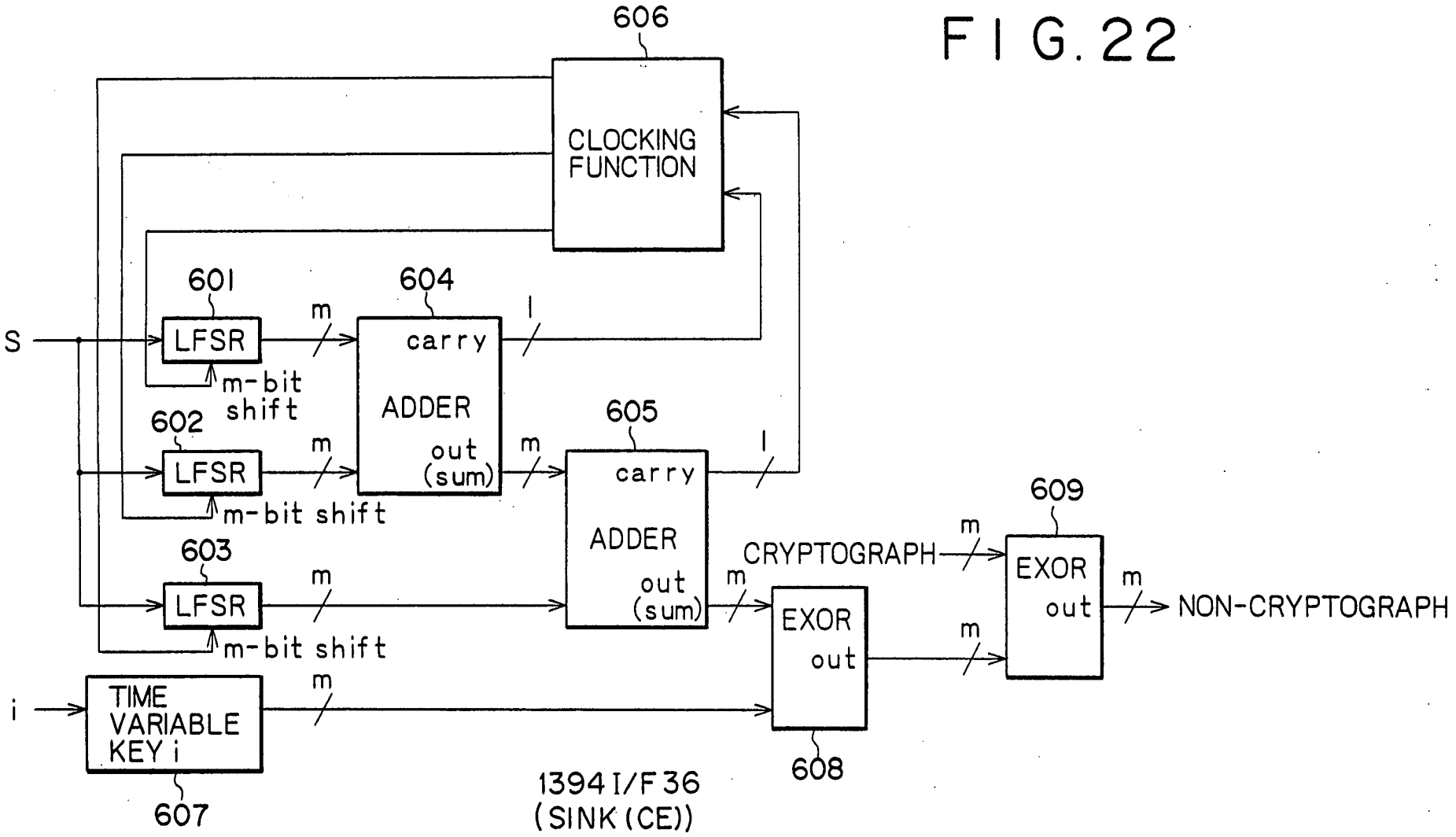
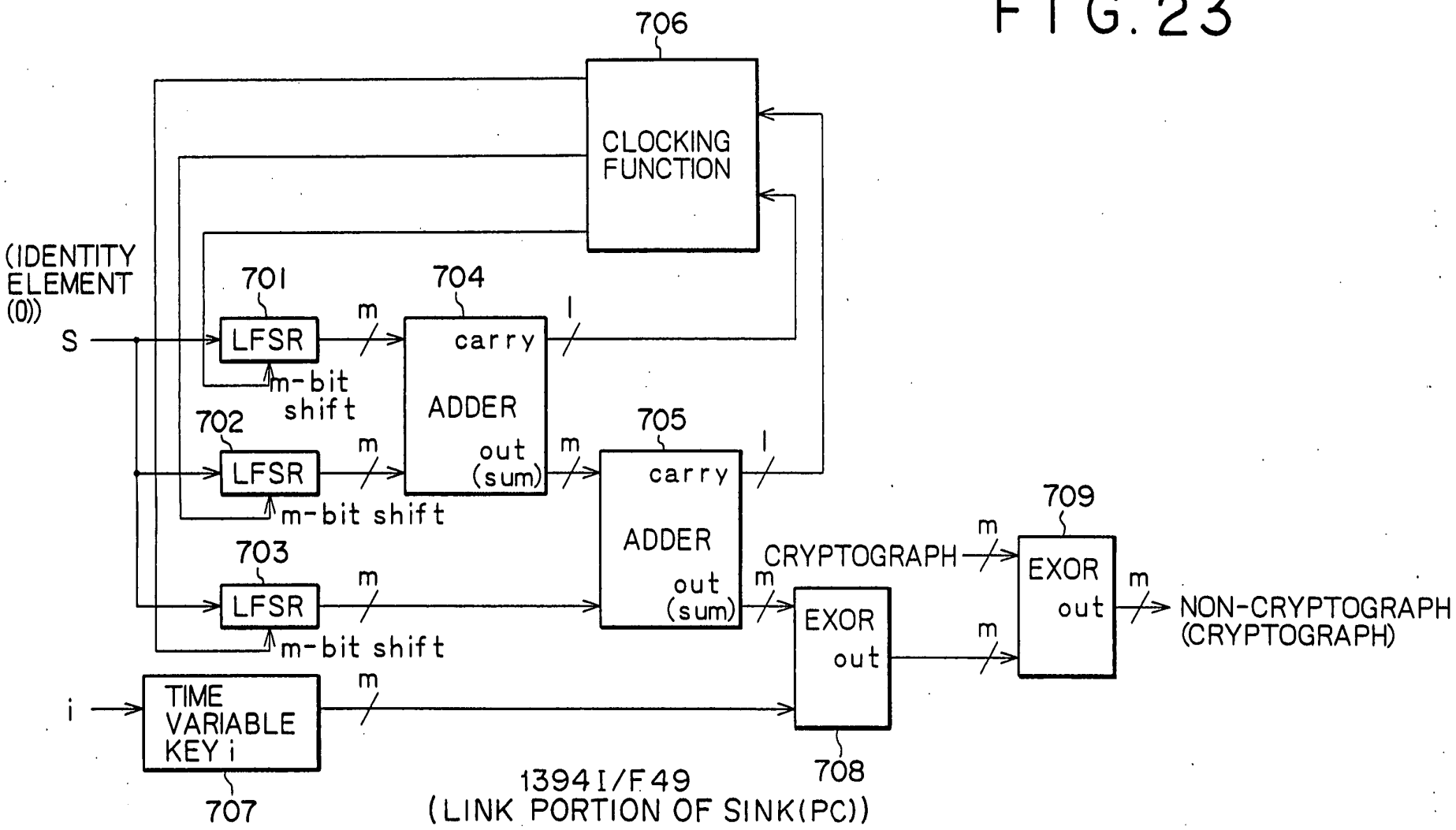


FIG. 23


706
CLOCKING FUNCTION
(IDENTITY ELEMENT (0))
S
701
LFSR
m-bit shift
704
carry
ADDER
out (sum)
m
l
702
LFSR
m-bit shift
705
carry
ADDER
out (sum)
703
LFSR
m-bit shift
709
CRYPTOGRAPH
EXOR
out
NON-CRYPTOGRAPH (CRYPTOGRAPH)
EXOR
out
i
TIME VARIABLE KEY i
707
1394I/F49
(LINK PORTION OF SINK(PC))
708

EP0090 6052860

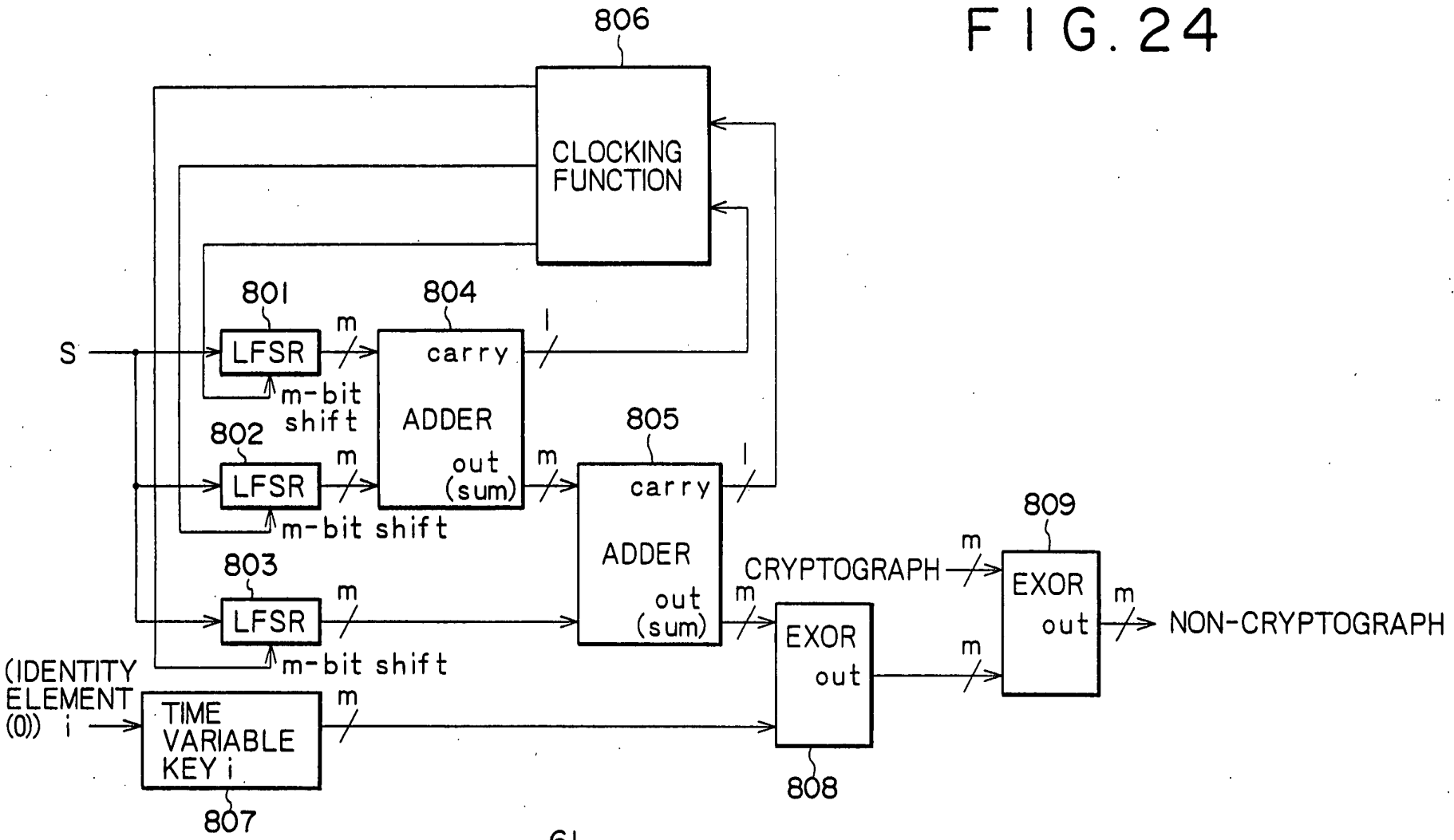



FIG. 24